(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2005 年8 月11 日 (11.08.2005)

PCT

(10) 国際公開番号
WO 2005/074215 A1

(51) 国際特許分類[7]: H04L 12/66

(21) 国際出願番号: PCT/JP2005/001524

(22) 国際出願日: 2005 年2 月2 日 (02.02.2005)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2004-025015 2004 年2 月2 日 (02.02.2004) JP
特願2004-267519 2004 年9 月14 日 (14.09.2004) JP
特願 2004-307953
2004 年10 月22 日 (22.10.2004) JP

(71) 出願人 (米国を除く全ての指定国について): 株式会社サイバー・ソリューションズ (CYBER SOLUTIONS INC.) [JP/JP]; 〒9893204 宮城県仙台市青葉区南吉成六丁目６番地の３ Miyagi (JP).

(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): キニ グレン マンスフィールド (KEENI, Glenn Mansfield) [IN/JP]; 〒9893204 宮城県仙台市青葉区南吉成六丁目６番地の３株式会社サイバーソリューションズ内 Miyagi (JP).

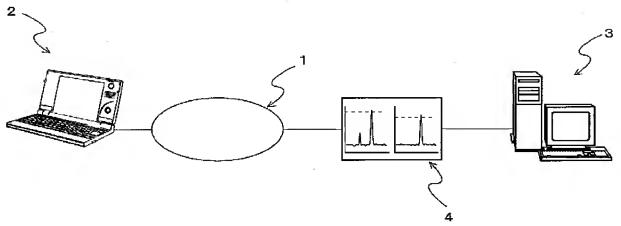
(74) 代理人: 福森 久夫 (FUKUMORI, Hisao); 〒1020074 東京都千代田区九段南４－５－１１富士ビル２Ｆ Tokyo (JP).

(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT,

[続葉有]

(54) Title: UNAUTHORIZED INFORMATION DETECTION SYSTEM AND UNAUTHORIZED ATTACK SOURCE SEARCH SYSTEM

(54) 発明の名称: 不正情報検知システム及び不正攻撃元探索システム




(57) Abstract: There is provided a system for detecting and tracing a (D)DoS attack and identifying the attack source, which system simplifies the judgment reference to determine whether a (D)DoS attack is present. The number of source addresses of the pockets transmitted via the Internet line is monitored. When the number of the source addresses has reached a predetermined number or a predetermined ratio within a predetermined time, it is judged that an unauthorized attack is present. Moreover, the packet of the HOP number different from the HOP number corresponding to the transmission source information is judged to be unauthorized information.

(57) 要約:

(D)DoS 攻撃であるか否かの判定基準を容易化することができる(D)DoS 攻撃検知および追跡、攻撃元特定システムを提供すること。

インターネット回線を通じて送信されてきたパケットのソースアドレスの数を監視し、ソースアドレスの数が一定時間内で所定数、若しくは所定率に達した場合には不正攻撃が行われていると判定することを特徴とする。

また、送信元情報に対応する HOP 数と異なる HOP 数のパケットは不正情報と判定する。

WO 2005/074215 A1

LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告書

２文字コード及び他の略語については、定期発行される各*PCT*ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

# 明 細 書

## 不正情報検知システム及び不正攻撃元探索システム

## 技術分野

[0001] 本発明は、インターネット回線を通じて送信されてきた情報が適正な情報であるかあるいは(D)DoSなどの不正な情報であるかを判定する不正情報検知システム及び不正攻撃元探索システムに関するものである。

## 背景技術

[0002] 特許文献1:特開2003−318987号公報

特許文献2:特開2003−234784号公報

[0003] 近年、ある企業や組織をターゲットにし、大量の不正な通信(パケット)を送信するサービス妨害攻撃が問題となっている。このような(D)DoS攻撃は、一般にはサーバの処理能力を超える大量の接続要求を一度に送りつけることや、通信回線の容量を不要な通信で埋め尽くすことで他の必要な通信を妨害し、通常業務を妨害したり、課金制ユーザーに対するプロバイダへのアクセス時間並びに通信会社への通信時間を延長させて納付料金を高騰させるといった弊害を与えるものである。いわゆる(D)DoS攻撃といわれるものである。

[0004] (D)DoS攻撃とは、攻撃対象機器およびネットワークの処理能力を上回る非常に甚大な数のパケットを送りつけ、対象のサービスを不能にしてしまう攻撃方法である。

[0005] そこで、各パケットのヘッダ部分に含まれるSourceアドレス(送信元アドレス)を管理し、このような(D)DoS攻撃を送りつけたアドレスからの通信を2度と受信しないと共にその送信元に通信の終了を示すパケットを送り返すといった防止機能を付加したサービスが見受けられる。

[0006] しかしながら、このような防止サービスは、異なったSourceアドレスから(D)DoS攻撃を送りつけてきた場合には、その(D)DoS攻撃の受信を拒否することができないといった問題が生じていた。

[0007] 一方、このような(D)DoS攻撃を送りつける送信元では、受信拒否された(D)DoS攻撃が送り返されてしまうと、自身のサーバおよびネットワークが容量オーバーとなってし

まう。

従って、送信元では、Sourceアドレスをランダムに偽造作成し、大量のパケットの各アドレスを異ならせたうえで特定宛先アドレスに(D)DoS攻撃を送信するといった対応で対抗してきているのが実情である。

[0008] これに対し、例えば、特許文献1では、不特定多数の電子メールに対し、電子メールのデータフォーマットのヘッダ部分に含まれるToアドレス(送信先アドレス)を事前設定されたアカウント別メールヘッダ・コンテンツ書き換え定義にしたがい、受信した電子メールを書き換えた上でその書き換えメールアドレスに再送信(転送)し、特定メールサーバーへの負荷を分散させている。

[0009] また、特許文献2では、同時に送信されてきた電子メールのFromアドレスに不明なものを大量に含むか否かを判定し、Fromアドレスに不明なものが大量に含まれている場合には、その送信されてきた大量の電子メールのFromアドレスに送信メールを返信し、返信できた電子メールのみを適正な電子メールとして受信している。

## 発明の開示

### 発明が解決しようとする課題

[0010] ところで、送信元アドレスは容易に偽造し変更することが可能であるため、大量の送信元アドレスを事前に予測し、対応することは非常に困難である。

[0011] また、(D)DoS攻撃は個々のパケットレベルでは正常な通信との区別が困難なことから、なんらかの閾値を用いた検知が検討されているが、それらは対象となるネットワークの特性や利用状況によって大きく変化するものであるため、高い検知精度は期待できない。

[0012] また、(D)DoS攻撃は正常な通信との識別が困難なことから、間違った判断により正常な通信の送受信をも遮断してしまう可能性があった。

[0013] このように、従来技術では、(D)DoS攻撃の判定基準が複雑となっているため、検知が困難な小規模の(D)DoS攻撃の受信を余儀なくされたり、必要な通信をも受信拒否してしまうといった問題が生じていた。

[0014] 本発明は、上記問題を解決するため、(D)DoS攻撃などの不正攻撃かあるか否かの判定基準を容易に行うことが可能な不正攻撃検知およびその追跡システムを提供す

ることを目的とする。

課題を解決するための手段

[0015] 請求項1に係る発明は、インターネット回線を通じて送信されてきたパケットのヘッダ内のあるフィールドの値の数を監視し、該フィールドの値の数が一定時間内で所定数、若しくは所定率に達した場合には不正攻撃が行われていると判定することを特徴とする不正情報検知システムである。

フィールドの値としては、例えば、次のものが上げられる。

バージョン

ヘッダ長

ToS

全長

アイデンティフィケーション

フラグ

フラグメントオフセット

Time to Live

プロトコル

ヘッダチェックサム

発信元アドレス

到達先アドレス

オプション

ポート

あるフィールドの値の数は、例えば、フィールドの値が「発信元アドレス」として、区別できる発信元アドレスとして、a1(＝一郎)、a2(＝二郎)、a3(＝三郎)、・・・・an(＝n郎)があった場合、フィールドの値の数はnである。

[0016] フィールドの値の数が、任意に決めた値の数以上になった場合に不正攻撃が行われていると判断する。任意の決めた値は、例えば、ある時点における数nt1に比較して他の時点における数nt2がk倍以上(kは例えば2以上の数)となったときに不正攻撃が存在すると決めてもよい。なお、フィールドの値の数が減少する場合にも不正攻

撃の存在があると判断する場合もある。

[0017] 請求項2に係る発明は、前記あるフィールド値のパケット数を監視することを特徴とする請求項1記載の不正情報検地システム。

[0018] フィールドの値の数fnとともにパケット数pmを監視し、その比で判断してもよい。ある時点における比(fn／pm)t1がある任意に決めた値以上になった場合に不正攻撃が存在すると設定してもよい。(fn／pm)t1と(fn／pm)t2との比がある値以上になったときに不正攻撃と判断してもよい。

[0019] 請求項3に係る発明は、前記フィールドの値は、複数のフィールドの組合せにより構成されていることを特徴とする請求項1又は2記載の不正情報検知システムである。

[0020] フィールドの値として「発信元アドレス」と「到達先アドレス」との組合せによりフィールドの値を構成する。

[0021] まず、前記同様、発信元アドレスとして、a1(＝一郎)、a2(＝二郎)、a3(＝三郎)、・・・・an(＝n郎)があったとする。

[0022] ak(k＝1ーn)について、到達アドレスの種類がmk個あるとすると、この場合における複数のフィールドの組合せにより構成されるフィールドの値の数はΣmk(k＝1ーn)となる。

[0023] 請求項4に係る発明は、インターネット回線上における、前記情報のホップ数が所定の値となった場合、若しくは特定のフィールドあるいはフィールドの組合せに該当するパケットの持つホップ数が変化した場合に当該情報を不正情報と認定することを特徴とする請求項1ー3のいずれか1項記載の不正情報検知システムである。

[0024] 請求項5に係る発明は、インターネット回線上における、前記情報のホップ数が所定の値となった場合、若しくは特定のフィールドあるいはフィールドの組合せに該当するパケットの持つホップ数が変化した場合に当該情報を不正情報と認定することを特徴とする不正情報検知システムである。

[0025] 請求項6に係る発明は、インターネット回線を通じて送信されてきたパケットのヘッダ内のあるフィールドの値の数を監視し、該フィールドの値の数が一定時間内で所定数、若しくは所定率に達した場合には不正攻撃が行われていると判定し、インターネットの複数個所で前記フィールドの値の数を監視することにより不正な送信元を探索

するようにしたことを特徴とする不正攻撃元探索システムである。

[0026] 請求項7に係る発明は、前記フィールドの値は、ヘッダ内の複数のフィールドの個々の組合せにより構成されていることを特徴とする請求項6記載の不正攻撃元探索システム。

[0027] 請求項8に係る発明は、インターネット回線上における、前記情報のホップ数が所定の値となった場合、若しくは特定のフィールドあるいはフィールドの組み合わせに該当するパケットの持つホップ数が変化した場合に当該情報を不正情報と認定することを特徴とする請求項7記載の不正攻撃元探索システムである。

## 発明の効果

[0028] 本発明の不正情報検知システムによれば、同時に大量に送信されてきたパケットに対し、その大量のパケットの値の数又はパケット数が一定時間内に所定数に達した時に、略同期して送信元アドレス件数が所定数若しくは所定率に達した場合には、その大量の電子メールを(D)DoS攻撃メールと判定することにより、特定の送信元アドレスに対して受信許可設定若しくは受信拒否設定をするといった細かく煩わしい設定をすることなく(D)DoS攻撃が送信されてきたことを認識および追跡することができる。

## 図面の簡単な説明

[0029] [図1]本発明の(D)DoS攻撃検知およびその追跡システムの概念図である。

[図2](A)はパケットデータフォーマットの説明図、(B)は通信量の一例を時系列で示したグラフ図、(C)はパケットのアドレス件数の一例を時系列で示したグラフ図である。

[図3]パケット探索を示す概念図である。

[図4]インターネットのシステムを示す概念図である。

## 符号の説明

[0030] 1…インターネット回線

2…送信側コンピュータ

3…受信側コンピュータ

4…通信監視装置(判定手段)

## 発明を実施するための最良の形態

[0031] 前述した通り、DoS攻撃とは、攻撃対象機器に処理能力を上回る非常に甚大な数のパケットを送りつけ、対象のサービスを不能にしてしまう攻撃方法である。
このDoS攻撃は次のような特徴を有している。

[0032] 例えば、ヘッダ内のフィールドの値の一つである発信元アドレスは偽造されている(偽のアドレスが用いられている)攻撃元の発信元
アドレスであるパケットをフィルタすることにより、DoS攻撃をブロックされないように、DoS攻撃の発信元アドレスはランダムに選択されていることが一般的である。

[0033] DoSは非常に莫大なパケットが送信されるので、次のような方法で検知される。

[0034] 第1の方法は、攻撃パケットもしくは、不正なパケットの数を数える方法である。どのようなパケットが不正であるかを判断することはむずかしい。なぜなら、DoS攻撃に使われるパケット一つ一つは正常なパケットであるからである。

[0035] 第2の方法は、検知したパケット全て(攻撃パケットも含む)を数える方法である。ネットワークトラフィックは時々刻々動的に変化する。従って、単にネットワークトラフィック量が増大したからといって、その現象はDoS攻撃によるものだと指摘することはできない。また、既にトラフィック量が飽和状態である場合は、DoS攻撃があったとしても、トラフィック量は増加しない。

[0036] それに対して、本形態における方法は、DoS攻撃の検知方法は、トラフィックの発信元アドレスを数える方法である。もし攻撃者がランダムに発信元アドレスを選択しているならば、観測される発信元アドレスの数も増加しているはずである。ある一定時間間隔では、1個の発信元アドレスに対して、そのような発信元アドレスを持つパケットは複数観測されるのが通常である。しかし、攻撃の最中では一般的に1個の(偽造された)発信元アドレスに対して、攻撃パケットは1個しか観測されない。このようにDoS攻撃を検知することができる。

[0037] 発信元アドレス、到達先アドレスとその他の情報・データから構成されている。時間間隔でパケットを数える。例えば、図3に示すように、ネットワーク(Net1)と攻撃先(Target)との間の経路にパケットを観測するための手段を設けておき、そこで、パケットを観測すればよい。かかる手段としては、例えばスニファー(Sniffer)やパッシブ型

プローブなどの機器がある。

[0038] スニファー(Sniffer)や、パッシブ型プローブなどの機器は全てのパケットを観測でき、それらの機器は以下の値を数えあげることができる。

パケットの全数

ある特定の発信元アドレスを持つパケット数

ある特定の到達先アドレスを持つパケット数

発信元アドレス毎のパケット数

到達先アドレス毎のパケット数

特定のタイプのパケット数

これらの値は、一定時間間隔毎に収集可能である。

[0039] 次にDos攻撃の追跡方法について述べる。

[0040] DoS攻撃元の追跡方法としては、第1に、不正なパケットの経路をチェックする(パケット追跡)方法がある。しかし、どのようなパケットが不正なのかを知る必要がある。

[0041] 第2に、トラフィックパターンをチェックする方法がある。しかし、この方法は、不正確である。

[0042] それに対して、本発明の実施の形態においては、経路上において観測されるアドレス数の変化をチェックする方法である。全ての経由地で同様な現象が観測されると推測される以下のようなパターンが観測される。

[0043]

| 時間(任意単位) | パケット数 | 発信元アドレス数 |
|---|---|---|
| 1 | 1000 | 50 |
| 2 | 800 | 60 |
| 3 | 900 | 57 |
| 4 | 1200 | 64 |
| 5 | 50 | 30 |
| 6 | 1500 | 530 |
| 7 | 1800 | 550 |
| 8 | 1700 | 570 |
| 9 | 800 | 80 |

10 900 65

上記において、時間6、7、8においては、パケット数とともに発信元アドレス数が増加している。そこでは、DoS攻撃がなされている。

[0044] 一方、図4に示すように、インターネットの各経路にスニファーSn(n＝1, 2, 3, ・・・)を置いておき、そこでの観測結果同士を比較すればどの経路でDoS攻撃がなされているかを知ることができる。その経路を遮断すればDoS攻撃元を追跡することができ、必要に応じてその経路を遮断すればよい。また、その経路からの所定のパケットを遮断すればよい。

[0045] なお、本発明において、フィールドの値としては、IPv4 プロトコルパケットを例にした場合、次のものが例示される。

バージョン領域
ヘッダ長領域
ToS 領域
全長領域
アイデンティフィケーション領域
フラグ領域
フラグメントオフセット領域
Time to Live 領域
プロトコル領域
ヘッダチェックサム領域
発信元アドレス領域
到達先アドレス領域
オプション領域
ポート領域

[0046] 本発明においては、これらのフィールドの個々の値の件数を検知してもよい。また、これらの個々のフィールドの値の2以上の任意の組合せをフィールドの値としてその件数を検知してもよい。

[0047] 以下に例を示す。

カテゴリは一つ、ないしは複数のヘッダ領域によって定められるパケットを分類できる性質のことである。

(カテゴリの例) プロトコル領域がTCPであるパケット全て

便宜上“Total カテゴリ”というカテゴリを定義する。全てのパケットはこのカテゴリに属する。

[0048] 今までの統計分析手法は、モニタや探査装置により観測されたパケットから、全ての観測パケット数や、あるカテゴリに対するパケット観測数などの標本値を元にしてきた。

[0049] [表1]

(例) プロトコル領域毎のパケット数

| | 全体 | TCPパケット | UDPパケット | ICMPパケット |
|---|---|---|---|---|
| 10:01 | 181 | 123 | 46 | 0 |
| 10:02 | 142 | 100 | 32 | 10 |
| 10:03 | 206 | 140 | 0 | 13 |
| 10:04 | 217 | 120 | 87 | 10 |

カテゴリ変換 (C-Transform) における統計分析では、検知したパケットが属するカテゴリの数に着目する。上記の例において、プロトコル領域ごとのカテゴリの数を見た場合以下の通りになる。

[表2]

| | 全体 | TCPパケット | UDPパケット | ICMPパケット | カテゴリの数 |
|---|---|---|---|---|---|
| 10:01 | 181 | 123 | 46 | 0 | 2 |
| 10:02 | 142 | 100 | 32 | 10 | 3 |
| 10:03 | 206 | 140 | 0 | 13 | 2 |
| 10:04 | 217 | 120 | 87 | 10 | 3 |

このようにパケットの数の分布からカテゴリの数の分布を作成する方法のことをカテゴリ変換“C-Transform” と呼ぶ。

[0050] いくつかのヘッダ領域の和によって作成されたカテゴリがとる事が可能な最大のカテゴリの数はその領域の合わせた幅による。例えば幅が合わせて4ビットの領域で作成される彼ごりの場合、最大のカテゴリの数は16個 (2の4乗) である。

[0051] しかし、IPヘッダにおけるVersion領域とProtocol領域のように、予め定義された以外の値を持つことができないヘッダ領域がある(ASSIGNED NUMBERS, RFC 790 参照)

。そのためこのような領域から作成できる意味のあるカテゴリは限定される。

[0052] また、32ビット(4294967296)の幅を持つ発信元アドレス、到達先アドレスのように非常に大きな値を取り得る領域からのカテゴリ変換 (C-Transform) は特に興味深い統計を提供することになる。

[0053] 本発明においては、インターネット回線上における、前記情報のカテゴリ数が所定の値となった場合に当該情報を不正情報と認定する。またホップ数を効果的に活用することで検知および追跡の効率を向上する。

[0054] (検知方法)

カテゴリ数、パケット数、通信量をそれぞれ以下のように定義する。1...iは時系列に並んだ値とする。

カテゴリ数： C1, .... Ci, ....

パケット数： P1, .... Pi, ....

通信量： O1, .... Oi, ....

このとき、以下の条件で検知する。

a. Ci >T

b. Ci / Ci+1 >T

c. Ci / {Pi|Oi} >T

T は閾値である

Tは固定値もしくはトラフィックデータから算出される値である

例えば、T = F X movingAverageOfStatistic ( in a, b, c above)

のように上記のa,b,cの値の移動平均になんらかの数Fを乗じて差出されたものである。

Fは固定あるいはトラフィックデータから算出される値である

例えば、F = A X standardDeviationOfStatistic

のように標準偏差を用いて算出されることもある。

Aは定数である

インターネットにおいては、情報の無限循環を防止するために、ヘッダのTTL(Time to Live)のフィールドの値に基づきHOP(ホップ)の数が0となったらその情報を

インターネット上から落とすことが行われている。ところで、ある送信元情報が示された場合、それが詐称されたものではなく正規の場合HOP数はほぼ決まっている。したがって、その決まっているHOP数と比較して、実際に送られた来た詐称情報の場合のHOP数が異なる場合その情報は不正情報と判断することができる。

## 実施例

[0055] 次に、本発明の(D)DoS攻撃検知およびその追跡システムの実施の形態を図面に基づいて説明する。

[0056] 図1は本発明の(D)DoS攻撃検知およびその追跡システムを示す図である。図1において、1はインターネット回線、2はインターネット回線1に接続された送信元のコンピュータ本体、3はインターネット回線1に接続された受信側コンピュータ、4はインターネット回線1と受信側コンピュータ3との間に接続された通信監視装置である。

[0057] 尚、この通信監視装置4はネットワークに接続されるが、受信側コンピュータ3がサーバー等であった場合には、そのサーバーを通信監視装置4としても良い。
この場合、受信とはサーバーで割り当てたポートに対する通信の受信を意味、判定のための受信は含まないものとする。また、受信側コンピュータ3がプロバイダ所有のメールサーバーであった場合には、他のインターネット回線を通じてメール受信端末(例えば、パーソナルコンピュータ等)が接続されることとなる。

[0058] 通常、送信側コンピュータ2から送信されるパケットは、図2(A)に示すように、その通信を構成するパケットのパケットデータフォーマット10のヘッダ部11に、送信元アドレスに相当するSourceアドレス12と送信先アドレス(受信側アドレス)に相当するDestinationアドレス13とが含まれている。

[0059] 通信監視装置4は、送信された値の数若しくはパケット数と、Sourceアドレス12の件数とを監視する。

[0060] 例えば、通常の送受信を想定した場合、送信元コンピュータ2から受信側コンピュータ3に送信される値の数は1件であり、例え、他の送信側コンピュータ(図示せず)から略同時期に他の通信が受信側コンピュータ3に送信されたとしても、その値の数とSourceアドレス12とは1対1で比例して増える。

[0061] また、例えば、特定の通常の通信が偶然大容量となることがあり得る。この場合、従

来の通信量に基づく検知では、その量だけを問題として、不正であると誤って判断されることがある。

[0062] この問題は、多くの通信が集まる人気のあるコンテンツを運用するサーバでは特に顕著な問題となり、通常の通信と(D)DoS攻撃を識別することが非常に困難となる。

[0063] このような場合、メール監視装置4では、図2(B)のピークP1に示すように、通信量としては通常の通信量よりも多い件数のパケットが送信されてきた判定する。

[0064] しかしながら、各パケットのSourceアドレス12は共通、あるいは特定のグループで占められることから、そのパケットを正式に受信する。尚、カテゴリ数が所定数以内であった場合(例えば、10件未満)に、その受信を許容するようにしても良い。

[0065] 一方、実際には1台の送信側コンピュータ2から送信されたパケットでありながら、送信元アドレス(Sourceアドレス12)をランダムに偽装して大量のパケットを受信側コンピュータ3に送信してきた場合、通信監視装置4では、図2(B)及び図2(C)のピークP2, P3に示すように、通信量(若しくはパケット数)が通常の通信の送受信のときよりも多くなると同時に、その各パケットのSourceアドレス12も略同時期に増大することになる。

[0066] 従って、通信量(若しくはパケット数)が所定数(例えば、100件)を越えた際、Sourceアドレス12の数も略同時期に所定数(例えば、90件)若しくは所定率(例えば、パケットの数に対して90%)を超えた場合には、その受信を拒否する。

[0067] 尚、このような一斉同時送信に対応した一定時間内に送信されてきた通信の件数(若しくはパケット数)の所定数並びにSourceアドレス数の所定数の設定は、サーバーの処理能力やネットワークの容量に応じたり、受信側コンピュータ3の所有者の業種等に応じたりして設定することができる。

[0068] 例えば、受信側コンピュータ3の所有者の業種がインターネット検索サービスやチケット販売等であった場合、多くの人の検索要求や人気のある旅行プランやイベント内容に対するアクセスが殺到するといったことが想定される。

[0069] 従って、これらの業種等では、日常的に通信量も多いことが想定できるため、その平均的な受信件数を考慮して所定値(件数等)を設定すればよい。

[0070] また、このようなアクセスが殺到した場合であっても、(D)DoS攻撃に相当するような

全く同じ時間（瞬間的）に大量の情報が送信されてくることは想定されるが、判定のための一定時間の設定を短くするといった設定変更でも対応は可能である。

[0071] また、不正攻撃元探索もできる。

[0072] また、特定のサーバが近隣にない、ネットワークの中間点であっても判定された不正攻撃先を割りだすことができる。（請求項9）

# 請求の範囲

[1] インターネット回線を通じて送信されてきたパケットのヘッダ内のあるフィールドの値の数を監視し、該フールドの値の数が一定時間内で所定数、若しくは所定率に達した場合には不正攻撃が行われていると判定することを特徴とする不正情報検知システム。

[2] 前記フィールド値の値の数とパケット数を監視することを特徴とする請求項1記載の不正情報検知システム。

[3] 前期フィールドの値の数と通信量(オクテット数／ビット数)を監視することを特徴とする請求項1記載の不正情報検知システム。

[4] 前記フィールドの値は、複数のフィールドの組合せにより構成されていることを特徴とする請求項1又は2記載の不正情報検知システム。

[5] インターネット回線上における、前記情報のホップ数が所定の値となった場合、若しくは特定のフィールドあるいはフィールドの組合せに該当するパケットの持つホップ数が変化した場合に当該情報を不正情報と認定することを特徴とする請求項1乃至4のいずれか1項記載の不正情報検知システム。

[6] インターネット回線上における、前記情報のホップ数が所定の値となった場合、若しくは特定のフィールドあるいはフィールドの組合せに該当するパケットの持つホップ数が変化した場合に当該情報を不正情報と認定することを特徴とする不正情報検知システム。

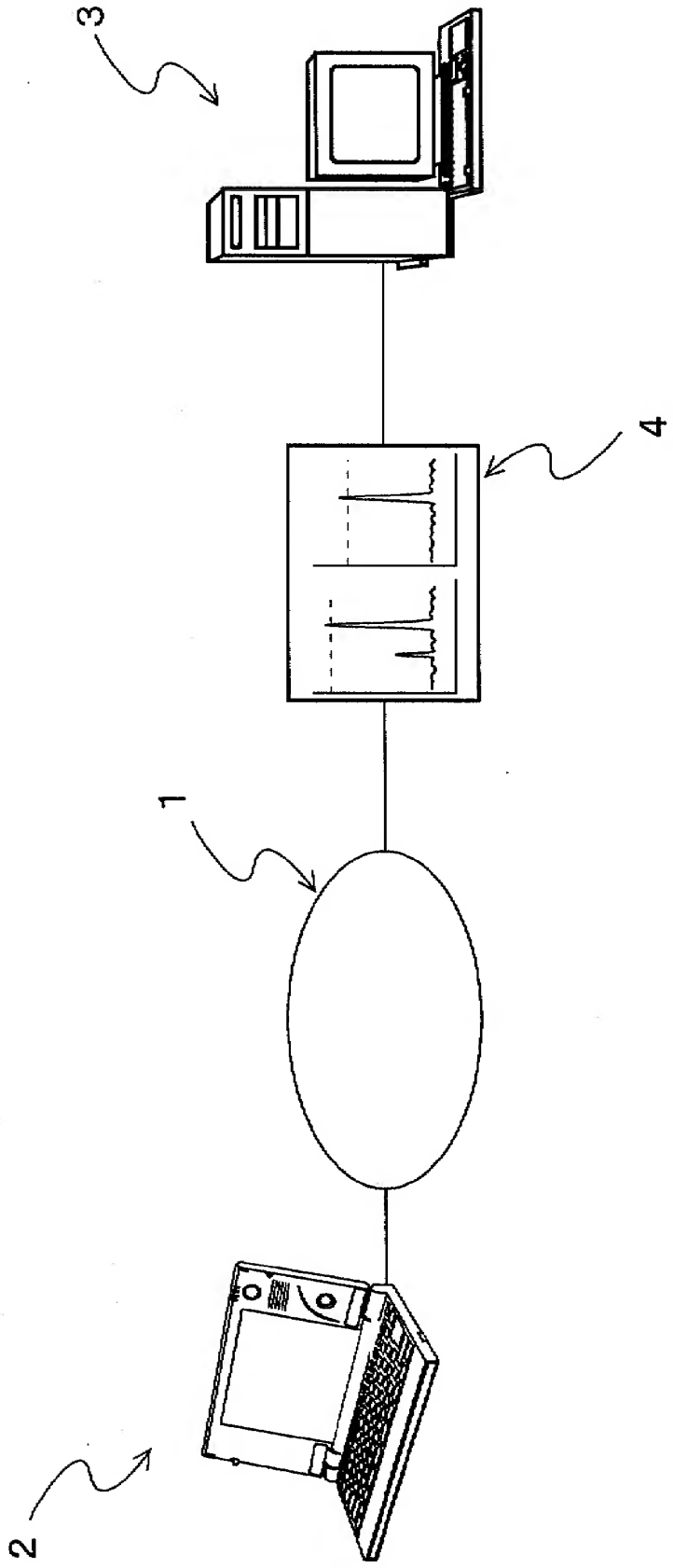
[7] インターネット回線を通じて送信されてきたパケットのヘッダ内のあるフィールドの値の数を監視し、該フィールドの値の数が一定時間内で所定数、若しくは所定率に達した場合には不正攻撃が行われていると判定し、
インターネットの複数個所で前記フィールドの値の数を監視することにより不正な送信元を探索するようにしたことを特徴とする不正攻撃元探索システム。

[8] 前記フィールドの値は、ヘッダ内の複数のフィールドの個々の組合せにより構成されていることを特徴とする請求項7記載の不正攻撃元探索システム。

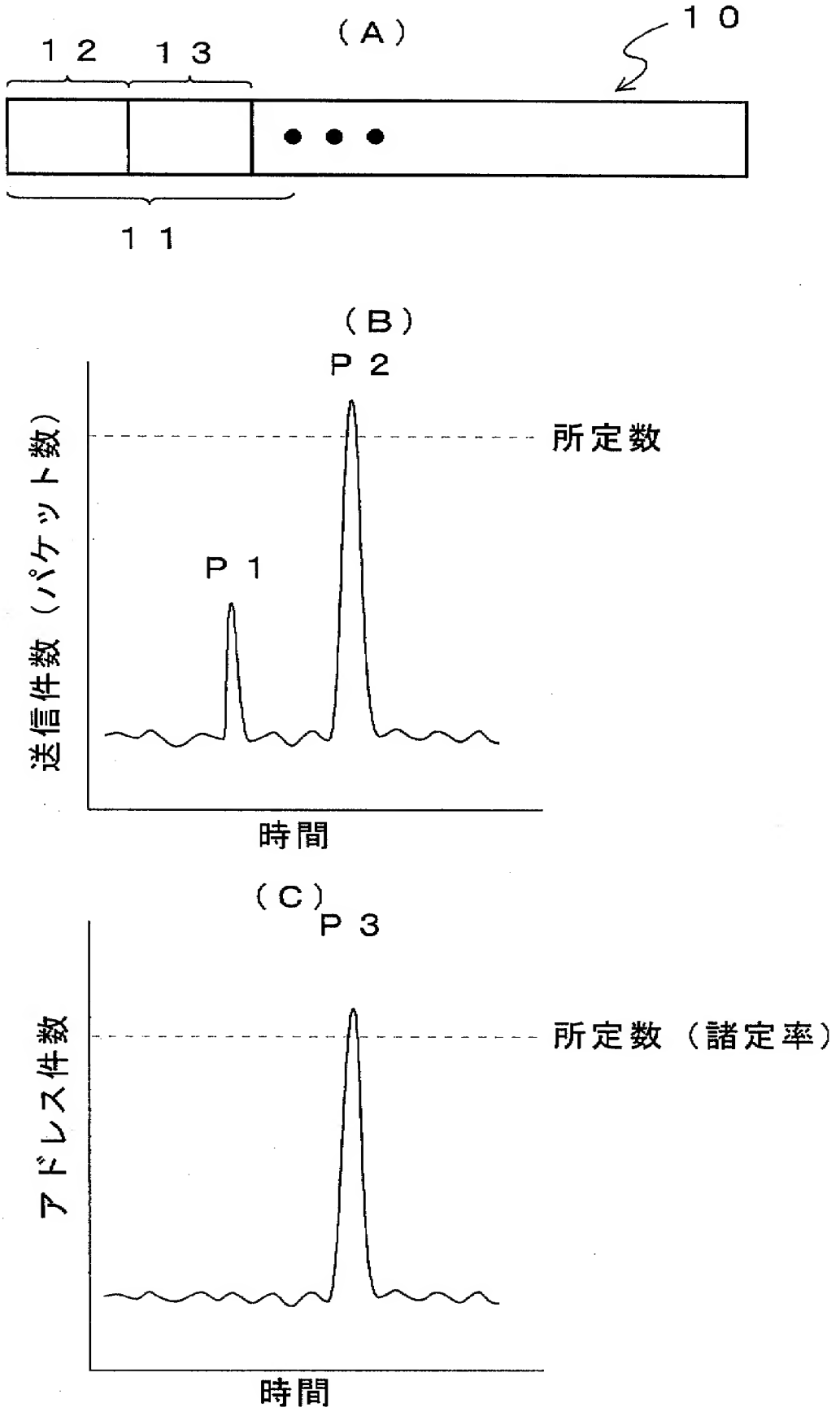
[9] インターネット回線上における、前記情報のホップ数が所定の値となった場合、若しくは特定のフィールドあるいはフィールドの組み合わせに該当するパケットの持つホッ

プ数が変化した場合に当該情報を不正情報と認定することを特徴とする請求項8記載の不正攻撃元探索システム。

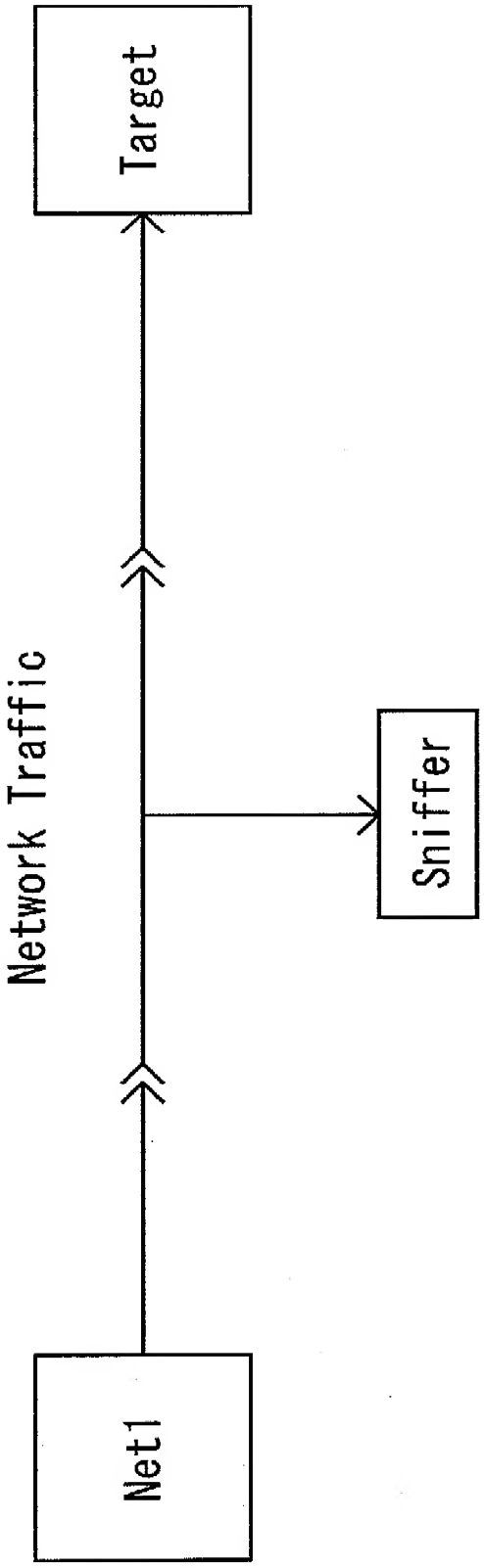
[図1]



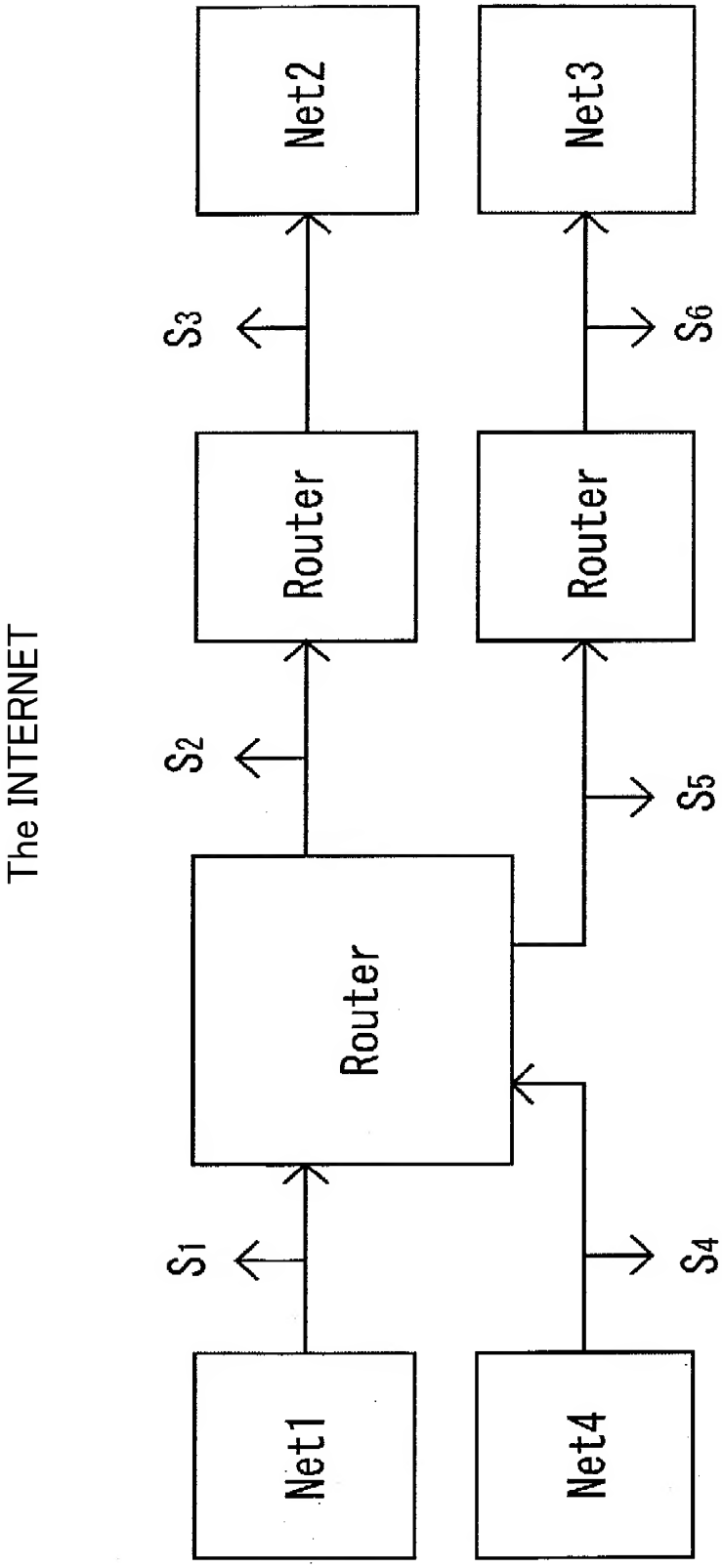
[図2]



[図3]



[図4]


The INTERNET
Net1
Net2
Net3
Net4
Router
Router
Router
S1
S2
S3
S4
S5
S6

# INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2005/001524

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] H04L12/66

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] H04L12/66

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
IEEE Xplore:DoS attack, DDos attack, source address

C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| X | JP 2003-283571 A (Nippon Telegraph And Telephone Corp.), 03 October, 2003 (03.10.03), Par. Nos. [0043] to [0049] (Family: none) | 1-9 |
| X<br>Y | JP 2004-140524 A (Sony Corp.), 13 May, 2004 (13.05.04), Par. Nos. [0044] to [0057] (Family: none) | 1-4<br>7,8 |
| X | WO 01/88731 A1 (NIKSUN INC.), 22 November, 2002 (22.11.02), & JP 2003-533925 A Claims 9 to 16 | 1 |

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

| Date of the actual completion of the international search | Date of mailing of the international search report |
|---|---|
| 02 May, 2005 (02.05.05) | 24 May, 2005 (24.05.05) |
| Name and mailing address of the ISA/<br>Japanese Patent Office<br><br>Facsimile No. | Authorized officer<br><br>Telephone No. |

Form PCT/ISA/210 (second sheet) (January 2004)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2005/001524

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| Y | Yosuke TAKEI, et al., "A Intrusion Detection and Trace using the Traffic Pattern" Technical Report of IEICE IN99-75, 18 November, 1999 (18.11.99) | 7,8 |
| A | Tatsuya OIKAWA et al., "Network anomaly Detection using Statistical clustering Method", Technical Report of IEICE IN 2002-87 24 September, 2002 (24.09.02) | 1-9 |
| A | JP 2002-252654 A (Mitsubishi Electric Corp.), 06 September, 2002 (06.09.02), (Family: none) | 1-9 |
| A | Tao Peng et al., "Protection form Distributed Denial of Service Attacks Using History-based IP Filtering", ICC'03 (11-15 May 2003), Vol.1, pages 482 to 486 | 1-9 |
| E,A | JP 2005-86452 A (Matsushita Electric Industrial Co., Ltd.), 31 March, 2005 (31.03.05), (Family: none) | 1-9 |

## INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2005/001524

**Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)**

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

**Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)**

This International Searching Authority found multiple inventions in this international application, as follows:

The inventions of claims 1-5, 7-9 relate to judgment of an unauthorized attack by monitoring the number of field values in a header of a packet.

The invention of claim 6 relates to judgment of an unauthorized attack by monitoring the hop number of a packet.

Upon judgment of an unauthorized attack, the inventions of claims 1-5, 7-9 should monitor a plurality of packets to decide whether an unauthorized attack is present while the invention of claim 6 can judge whether an unauthorized attack is present by monitoring only one packet. That is, these judgments of the unauthorized attack are different. Accordingly, these inventions are not so linked as to form a single general inventive concept.

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. ☒ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

**Remark on Protest**

☐ The additional search fees were accompanied by the applicant's protest.

☐ No protest accompanied the payment of additional search fees.

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２００５／００１５２４

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.[7]　H04L12/66

Ｂ．　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

Int.Cl.[7]　H04L12/66

最小限資料以外の資料で調査を行った分野に含まれるもの

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

IEEE Xplore : DoS attack, DDos attack, source address

Ｃ．　関連すると認められる文献

| 引用文献のカテゴリー＊ | 引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示 | 関連する請求の範囲の番号 |
|---|---|---|
| X | JP 2003-283571 A(日本電信電話株式会社)2003.10.03(ファミリー無し)【0043】～【0049】 | 1-9 |
| X<br>Y | JP 2004-140524 A(ソニー株式会社)2004.05.13（ファミリー無し）【0044】～【0057】 | 1-4<br>7,8 |
| X | WO 01/88731 A1(NIKSUN INC.)2001.11.22 & JP 2003-533925 A Claim 9～16 参照 | 1 |

☑ Ｃ欄の続きにも文献が列挙されている。　☐ パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「Ａ」特に関連のある文献ではなく、一般的技術水準を示すもの
「Ｅ」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「Ｌ」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「Ｏ」口頭による開示、使用、展示等に言及する文献
「Ｐ」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「Ｔ」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「Ｘ」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Ｙ」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「＆」同一パテントファミリー文献

| | |
|---|---|
| 国際調査を完了した日<br>０２．０５．２００５ | 国際調査報告の発送日　24.5.2005 |
| 国際調査機関の名称及びあて先<br>日本国特許庁（ＩＳＡ／ＪＰ）<br>郵便番号１００－８９１５<br>東京都千代田区霞が関三丁目４番３号 | 特許庁審査官（権限のある職員）　5X　9077<br>吉田　隆之<br>電話番号　０３－３５８１－１１０１　内線　３５９６ |

様式ＰＣＴ／ＩＳＡ／２１０（第２ページ）（２００４年１月）

Ｃ（続き）．　関連すると認められる文献

| 引用文献のカテゴリー＊ | 引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示 | 関連する請求の範囲の番号 |
|---|---|---|
| Y | Yohsuke Takei et.al.” A Intrusion Detection and Trace using the Traffic Pattern” Technical Report of IEICE IN99-75(1999.11.18) | 7,8 |
| A | Tatsuya OIKAWA et.al” Network anomaly Detection using Statistical Clustering Method” Technical Report of IEICE IN2002-87(2002.09.24) | 1-9 |
| A | JP 2002-252654 A(三菱電機株式会社)2002.09.06（ファミリー無し） | 1-9 |
| A | Tao Peng et.al.” Protection form Distributed Denial of Service Attacks Using History-based IP Filtering” ICC’03 (11-15 May 2003) Vol.1 P482-486 | 1-9 |
| E,A | JP 2005-86452 A(松下電器産業株式会社)2005.03.31(ファミリー無し) | 1-9 |

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２００５／００１５２４

第Ⅱ欄　請求の範囲の一部の調査ができないときの意見（第１ページの２の続き）

法第8条第3項（ＰＣＴ17条(2)(a)）の規定により、この国際調査報告は次の理由により請求の範囲の一部について作成しなかった。

1．☐ 請求の範囲＿＿＿＿＿＿＿＿＿＿ は、この国際調査機関が調査をすることを要しない対象に係るものである。
つまり、

2．☐ 請求の範囲＿＿＿＿＿＿＿＿＿＿ は、有意義な国際調査をすることができる程度まで所定の要件を満たしていない国際出願の部分に係るものである。つまり、

3．☐ 請求の範囲＿＿＿＿＿＿＿＿＿＿ は、従属請求の範囲であってＰＣＴ規則6.4(a)の第２文及び第3文の規定に従って記載されていない。

第Ⅲ欄　発明の単一性が欠如しているときの意見（第１ページの３の続き）

次に述べるようにこの国際出願に二以上の発明があるとこの国際調査機関は認めた。

請求の範囲１～５，７～９はパケットのヘッダ内のあるフィールドの値の数を監視することにより不正攻撃を判定するものである。
請求の範囲６はパケットのホップ数を監視することにより不正攻撃を判定するものである。

請求の範囲１～５，７～９は不正攻撃の判定に際して、複数のパケットを監視しなければ不正攻撃かどうか判定できないが、請求の範囲６は、１つのパケットだけを監視して不正攻撃かどうか判定できるものであるから、これらの不正攻撃の判定は、異なる判定を行うものであり、単一の一般的発明概念を形成するように連関する一群の発明であるとは認められない。

1．☐ 出願人が必要な追加調査手数料をすべて期間内に納付したので、この国際調査報告は、すべての調査可能な請求の範囲について作成した。

2．☑ 追加調査手数料を要求するまでもなく、すべての調査可能な請求の範囲について調査することができたので、追加調査手数料の納付を求めなかった。

3．☐ 出願人が必要な追加調査手数料を一部のみしか期間内に納付しなかったので、この国際調査報告は、手数料の納付のあった次の請求の範囲のみについて作成した。

4．☐ 出願人が必要な追加調査手数料を期間内に納付しなかったので、この国際調査報告は、請求の範囲の最初に記載されている発明に係る次の請求の範囲について作成した。

追加調査手数料の異議の申立てに関する注意

☐ 追加調査手数料の納付と共に出願人から異議申立てがあった。

☐ 追加調査手数料の納付と共に出願人から異議申立てがなかった。